bitcoin

Made Easy For Non-Geeks

Contents

Published By **Mark Maffei**

Table Of Contents

Legal Notices

Copyright Notice

Accuracy of Information

The Publisher of this report has taken reasonable measures to ensure the accuracy of the information contained herein. However, due to the rapidly-evolving nature of cryptocurrencies and legislation, this does not guarantee its accuracy; whereby the Publisher will not accept liability for any loss or damage which may arise directly or indirectly from the content contained herein.

This report is subject to change at any time without notice, and is provided on an "As-Is" basis for educational and entertainment purposes only as general cryptocurrency commentary. Its purpose is to assist cryptocurrency investors in making independent investment decisions.

Information contained herein does not constitute investment advice. The author will not accept liability for any loss or damage, including without limitation to, any loss of profit, which may arise directly or indirectly from use of or reliance on such information. Therefore *exercise due diligence* when any reasonably prudent person would do so.

Risk Disclosure

Past results are not necessarily indicative of future gains.

The risk of loss in cryptocurrency investing can be substantial and may not be suitable for all investors.

Carefully consider the inherent risks of such an investment in light of your financial condition, investment objectives, level of experience, and risk appetite. Avoid investing money that you cannot afford to lose. Be aware of all the risks associated with cryptocurrency exchange trading, and seek advice from an independent financial advisor if you have any doubts.

Furthermore, there are also risks associated with utilizing an Internet-based deal execution trading system including the failure of hardware, software, and Internet connection.

Since cryptocoin exchanges do not control signal power, its reception or routing via Internet, configuration of your equipment or reliability of its connection, they cannot be responsible for communication failures, distortions or delays when trading via the Internet.

Simply Stated: Your liability is *yours and yours alone.*

Pt. 1: Bitcoin Essentials Made Refreshingly Simple!

Brief Introduction

"In essence, Bitcoin's success is due to the fact that the man in the street understands that central banks and governments are going to take their money via confiscation or default or devaluation and it is their way of voting against it and them (since gold is not easily exchangeable for them). This is the 99% sticking their fingers up at the authorities and saying we don't need you or want you..."

- Raoul Pal

So what exactly is Bitcoin, minus the techno-babble?

The Short Answer: Bitcoin is an revolutionary decentralized digital currency (aka "cryptocoin", "cryptocurrency") and store-of-value investment instrument specifically made for the web; the digital counterpart of gold (with Litecoin being the digital counterpart of silver).

Bitcoin enables direct peer-to-peer payments to anyone, anywhere in the world via the **blockchain**.

The blockchain is a public ledger of Bitcoin's *entire transaction history* since going live, and is available for perusal by anyone 24/7; whereby creating a viable alternative to fiat banking snakery.

The Slightly Longer Answer: Bitcoin is an open source innovation based on the mathematics of public-key cryptography; originally inspired by an article written in 1998 by Wei Dai that envisioned the concept of cryptocurrency called "B-money".

However, it was actually first created by a mysterious individual or group that went by the moniker "Satoshi Nakamoto"; released to the general public in early 2009, under the MIT open source license.

Instead of having to trust some highly centralized third party payment gateway that can do you dirty with no warning whatsoever... mining new bitcoins and managing Bitcoin transactions are carried out collectively by via a peer-to-peer distributed network (think along the lines of BitTorrent or Napster).

To this day, all of the most time-proven and highly-respected cryptocoins still take a decentralized and open approach; and do so in a *provably fair way* without the need of a central authority.

To process, verify and archive payments, Bitcoin uses a unique combination of a public ledger (i.e. its blockchain), peer-to-peer networking, and a proof-of-work protocol (**PoW)** by "Bitcoin mining" via what basically amounts to solving complex cryptographic puzzles.

Hence bitcoins are essentially cryptographically signed over in the background from one wallet address to another. In turn, each payment transaction is broadcast across the network and forever added to the blockchain; whereby keeping everything provably fair (unlike traditional fiat banking snakery).

PoW vs. PoS

Long to short, PoW-based coins like Bitcoin and Ethereum are *extremely resource-hoggish* and burn a LOT of electricity; conversely PoS-based coins ("proof-of-stake") are **several orders of magnitude** more energy-efficient; to the extent of being **green** (a mere *fraction of a fraction* of a kilowatt per transaction).

Moreover, **PoS-based** cryptocoins:

- Have MUCH lower TX fees than Bitcoin.
- Can be mined with an *old antiquated computer* lying around collecting dust (oftentimes even a **Raspberry Pi**, for that matter).

To put this into perspective, Bitcoin is SO energy hoggish that it is quickly approaching a whopping **1 megawatt** of power *per individual transaction* (960 KW/transaction at this writing). Yikes! Here's a complete breakdown of Bitcoin's insane power consumption.

Bitcoin Fee Structure Demystified

Once there is at least 1 miner confirmation of a transaction, those bitcoins are *extremely difficult* to spend twice in a row back-to-back (called a "double spend").

Each additional miner confirmation makes it *exponentially more difficult* to double-spend.

Upon rendering the transaction fee to the network miners (aka "TX fee"), the first confirmation is initiated. Generally speaking, within 0.5-2 hours, each BTC transaction *is initially confirmed* onto the blockchain (altcoins are typically **way faster**).

However, heavy network congestion can actually make a Bitcoin transaction take MUCH longer than usual (such as was experienced throughout December 2017, when BTC hit an all-time high of ~$20K).

Another huge determining factor is the TX fee *set by the sender*.

A Good Analogy: The U.S. Mail System

When you send a parcel, you have numerous mailing options. Typically speaking, the more you're willing to pay, the faster your package arrives. In this regard, miners *will always move the transactions with the most attractive TX fees first* (i.e. most expensive, from the sender's point of view).

The lower a sender sets their TX fee, the longer their transaction will take to get registered onto the blockchain. Some transactions have been known to get stuck for days, because the TX fees offered were too low.

Personally, I'd rather pay the "Priority Mail" TX fee **and know** my transaction will get pushed onto the blockchain *in a timely manner*… but that's just me; your mileage may vary.

Honest Money

[The following short excerpt is from "*Bitcoin: What It Is and Why It Matters*", by Anthony Freeman]

"Honest Money (defined as a medium of exchange consisting of real goods that are in limited supply) can actually increase in value over time. Let me explain.

When the production of other economic goods grows at a faster rate than the supply of money (mined gold for example) the money can buy (be traded for) more of these other goods (money supply divided by the total number of goods).

This means that it could actually pay to save your money because it can increase in exchange value over time. This also means that nominal wages could decrease over time while real wages increase (your paycheck "amount" drops but your purchasing power increases).

Why and how did Government Money supplant Gold and Silver? Laziness and deceit. The first bankers were the goldsmiths. miners would bring the gold to the goldsmiths for minting. The goldsmith would give the miner a receipt that he could redeem when the minting was completed.

The miner soon found that he could immediately trade his receipt (his claim on the gold) for tools and supplies and return to the mines without having to wait for his gold. Over time, the goldsmith found that the receipts he issued stayed in circulation and were being used as medium of exchange. Only a small percentage of the people ever came in to redeem the receipts.

To increase his purchasing power he simply began to issue his own fraudulent receipts (that had no gold backing) and used them to acquire goods and services. This increase in the number of outstanding receipts created inflation and lessened the value of all of the other outstanding receipts.

In later days, central banks did the same thing. They issued more receipts (paper currency) than they had the gold and silver to back it. The U.S. paper currency was originally a receipt for gold or silver. "

Points To Ponder:

- Cryptocurrencies provide an open, honest and reliable payment network (unlike fiat currencies which are government-controlled, debt-based, and inflated at will).

- Cryptocurrencies store real value. In other words, the *most your fiat currency* will ever be worth is whatever it's worth right now today. This is because fiat currency can be "printed" at the mere push of a button (or worse yet… an engineered crash at some point).

- The value of 1 BTC has gone from US$0.03 (yes, three pennies) per Bitcoin in February 2009, to a **staggering ~$20K** briefly in December 2017; its overall trend for the last 9 years has been "To the moon!". According to a conservative estimate by Cameron Winklevoss (co-founder of the highly popular FDIC-insured exchange Gemini), he conservatively estimates that BTC will reach at least $40K per bitcoin.

Important Crypto-Wallet Considerations

Often times you'll see some online biz trying to get people to sign up for their free crypto-wallet or download their wallet app. Do so with **extreme caution**; because here's what they oftentimes neglect to mention to the unsuspecting crypto-newbie: *Whoever controls your private keys controls your cryptocoins.*

Allow me to briefly explain.

ALL Bitcoin wallets (and nearly all crypto wallets in general) simply consist of 2 cryptographic "keys":

- **A public key** (aka "public wallet address"). This is the one *you share to receive funds.*
- **A private key** (the one that unlocks your wallet). This is the one *you must diligently safeguard against prying eyes*. If some unscrupulous douchebag discovers your private keys and steals your coins… you're straight-up **screwed**, as there is zero way to retrieve them!

A Brief Word On Online Wallets

These wallets require zero downloading/installing of any type of software, whatsoever.

Pro:

- **Convenience:** Aimed at Bitcoin newbies, the best attribute of an online client is the sheer convenience of logging in anytime, anywhere, on any device.

Con:

- **Tend To Be Less Secure:** Desktop wallet clients that value *private key sovereignty* (i.e. you are exclusively in control of your private keys at all times, such as with Exodus) tend to offer superior BTC security, as evidenced by this horrific case example.

Summary:

While online clients should generally be avoided altogether… the only one I can comfortably recommend is the highly vaunted Blockchain wallet; which has thus far proven to be a reputable company that actually gives a crap about its users.

Nonetheless, I cannot strongly enough advise you to grab the Exodus wallet specific to your OS (covered in Part 2) as your primary multi-coin wallet; whereby only using Blockchain as an "online spending" wallet (if at all, as Exodus is superior in every regard and such a pleasure to use).

Cryptocoin Security Tips

Cryptocoins make it possible to transfer value anywhere very easily and maintain financial sovereignty over your own money. However, *with such power comes great responsibility*. Hence it's in your own best interests to protect your cryptocoins as you would anything valuable you wouldn't want stolen.

What follows is numerous tips to keep your cryptocoins where they belong… in YOUR possession!

Wallet Security Quick Tips

- Treat your cryptocoins and wallets *with the same care* as you would hard cash, purses, and wallets.

- Back up your wallet private keys in at least two *secure locations*. A safely-stored backup of your private keys and wallet passphrases (a randomly-generated string of 12 words) can protect you against both computer failures and a myriad of human mistakes.

- Make sure you never lose/forget wallet passphrases or your funds will be **permanently lost**. If in doubt, keep a hard copy of your password in a safe place like a vault.

- Consider using different storage media types for your wallet key your backups (i.e. encrypted USB sticks, physical paper, encrypted CDs, etc.)

- Offline wallets are best for long-term saving. Offline wallets (aka 'cold storage' paper wallets provide the highest level of security for *large scale long-term investing*. It entails storing a wallet in a non web-connected manner. When done properly, it can offer excellent protection against a wide range of digital and human vulnerabilities.

- Always keep your wallet client app software up to date; whereby staying current on important stability, security and bug fixes (as well as any new features introduced).

Cryptocoin Power User Anonymity & Privacy Tips

Perhaps you've heard the hype about Bitcoin being 'anonymous'. Actually, that's only half true; and as we all know: "*Half a truth is worse than a lie.*"

In reality, blockchains are the most transparent transaction networks in the world. Yet at the same time, they can also provide impressive levels of anonymity and privacy *when used correctly* (particularly with "privacy coins" like Zcash or Monero).

Along the same lines as the extra precautions you'd take when doing online banking... cryptocurrency is just as serious (and in certain regards, even more so). It's all about being *exceptionally discreet* when attached to the web.

What follows is some great tips to enhance your overall anonymity, privacy and security.

- **Understand Bitcoin traceability.** Bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. All bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network.

Conversely, Bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent. These addresses are created privately by each user's wallet. Once addresses are used, they become tainted by the history of all transactions they are involved with. Moreover, anyone can see the balance and all transactions of any address.

Sometimes users will have to reveal their identity in order to receive certain goods and services; hence Bitcoin addresses cannot remain anonymous under these circumstances. Consider using a "one and done" disposable wallet address for these purposes.

- **Use new addresses to receive payments.** For maximum privacy, you should generate a new Bitcoin address each time your receive a new payment (including any change owed to you - covered below).

- **Use multiple wallets for different purposes.** Doing so allows to isolate each of your transactions in such a way that it is virtually impossible to associate them all together. People who send you money cannot see what other Bitcoin addresses you own and what you do with them. This is very important advice to keep in mind.

- **For added anonymity, use "change addresses" if possible.** Certain wallet clients (such as bitcoin-Qt) make it difficult to track your outgoing transactions by creating a new change address each time you send a payment. For example, if you receive 5 BTC on address A, and you later send 2 BTC to address B, the remaining change must be sent back to you.

- **Be careful with public usage.** Unless your intention is to receive *public donations or payments with full transparency*, publishing a bitcoin address on any public space (i.e. blog, social media, etc.) is not a good idea when it comes to privacy.

Generally speaking, when you move coins from a publicly posted address to one of your non-public wallets, those coins will be permanently tainted *via the blockchain history* of your publicly posted address. Additionally, it's wise not to publish information about your transactions and purchases that could allow someone to identify your coin addresses.

- **Your IP address is most likely being logged.** Because cryptocoin networks are peer-to-peer, it’s entirely possible to listen for relayed transactions and log their IP addresses.

Full node clients relay all users' transactions just like their own. This means that finding the source of any particular transaction can be difficult and any coin node can be mistaken as the source of a transaction when they are not.

Consider masking your computer's IP address with a tool like Tor to help you avoid these undesirable logging issues. Further exercise due diligence when surfing, along with these 10 Ways to Boost Firefox Privacy.

Closing Thoughts Before Moving To The Next Section

Some online services called “coin mixing” services offer to mix traceability between users by receiving and sending back the same amount using independent addresses. The legality of using these “coin mixing” services is *highly dubious*; varying greatly from jurisdiction to jurisdiction (in terms of legal ramifications/penalties).

At best, such practices are **always considered sketchy** by the Powers That Be. Also, these types of services require you to put an *extreme amount of blind faith* in the service, hopin’ and a prayin’ that your coins will not be stolen (not to mention the server log left behind of your coin-mix requests).

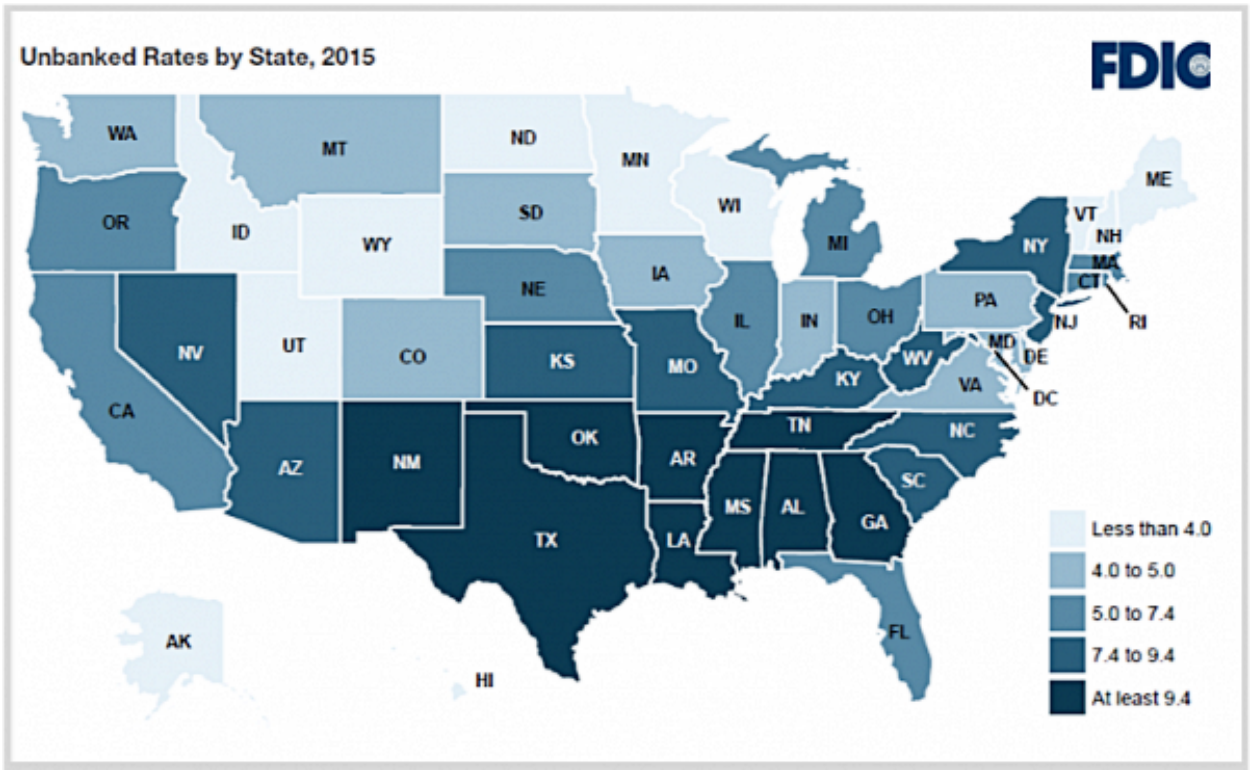
You’re far better off simply converting your BTC into one of the “anonymity cryptocurrencies”; then back into BTC via a *completely different address* than the origin address.

Last but certainly not least… save the “Data Dealer: Legal? Illegal? Whatever” PDF to a convenient location and *absorb it’s chillingly sobering ramifications at your earliest leisure* (preferably with a tasty beverage of choice in hand). It definitely inspires a profound sense of **healthy paranoia**.

Pt. 2: Smoothly Transitioning Into Crypto

Brief Overview

There is an exodus from fiat tyranny quietly going on behind the scenes. Moreover, well over half our planet is underbanked and approximately one third of it is unbanked. And it's not just "developing countries" that are underbanked or unbanked:



It's no wonder why cryptocurrencies finally went mainstream in 2017, and have continued exploding in popularity with no let-up in sight. To help further augment this amazing global phenomena, the wildly popular **Exodus multi-cryptocoin wallet** has *greatly lowered the technological barriers to entry* historically holding non-geeks back from getting in on the action:

- **User-Friendliness:** Exodus was built *from the ground up* with the unique needs of crypto-newbies in mind (not merely a post-release afterthought).

- **Intuitive Interface:** Combing the very best in both ease of use AND sheer elegance, the stunningly beautiful Exodus GUI actually *makes it highly pleasurable* to check up on your crypto investments throughout the day.

- **Robust Coin Support:** At the time of this writing, Exodus has already integrated over 30+ popular cryptocoins (plus *several popular Ethereum tokens* as well), and are constantly in the process of vetting new assets for future inclusion.

- **Passionately Proactive Development:** The Exodus dev team takes wallet safety *hardcore seriously* and is right on top of their bug-fixes as necessary.

- **Attractive Themes:** Exodus has lots of beautiful themes to choose from; whereby making it a breeze to switch between themes as the mood requires.

- **Sovereign Private Key Ownership:** Your private wallet keys are *yours and yours alone*; whereby remaining in YOUR possession at all times!

- **Amazing Customer Support:** While researching the Exodus information contained herein, I had to contact customer support several times in order to confirm information accuracy. The customer support was a*lways quick and courteous* without fail.

- **Convenient Crypto Asset Transportation:** Exodus makes it *highly convenient* to move your crypto assets in and out of Exodus/

- **Best Tx-Fee-to-Transaction-Speed Ratio Possible:** Exodus is specifically set up to fetch the best TX fee at point of transaction (based on real-time network traffic). This ensures that your Exodus transactions always receive priority confirmation on the blockchain *at the best TX fee possible.*

- **Delightfully Simple Built-In Coin Converter:** Exodus even has a *delightfully simple coin exchanger built right in*; so you don't even have to leave the comfort of your own wallet to enjoy "down and dirty" cryptocoin conversions 24/7 on the fly:

The Exodus Edge

Exodus is wholeheartedly supportive of every individual's right to *privacy and sovereignty over own their funds*. They've incorporated these principles into the Exodus wallet from the very beginning.

For example, your bank account or stock portfolio holdings are not actually yours so long as they are "managed" by another entity; likewise with certain crypto wallets you do not exclusively maintain the private keys. Said another way, unless you have **100% control** over your money and investments (whether fiat or crypto)… *then someone else does*.

Putting this level of trust in highly-centralized banks and companies "supposedly" acting in your best interest ultimately exposes you to several layers of unnecessary risk; whereby your funds can be *ganked without warning*… Mt. Gox, BTC-e, Payza, Argentina, Greece… Poof! Gone.

Conversely, Exodus (the company) has *zero access to any of your wallet assets*. You are in **100% control** of your own assets through a set of private keys generated the very first time you open your Exodus wallet.

In this regard, Exodus *fundamentally differs* from big highly-centralized exchanges like Coinbase or Bittrex. In essence, they are just glorified centralized bank accounts in which you are given the equivalent of "casino credits" proportional to the money you deposit.

While sitting on these centralized platforms, those cryptocoins are not really yours until they are back home safe and sound in a wallet *you have control over the private keys*. With Exodus **YOU** and you alone are always in 100% control of your own private keys at all times!

Private Keys: The Key To Controlling Your Financial Future

Not to be confused with your *12-word mnemonic backup phrase*, the main thing to understand is that private keys are the **#1 most important** factor in controlling your financial future.

Exodus wrote a great article that will help you to understand and locate your private keys on the computer containing your Exodus wallet.

For even greater security and privacy, Exodus connects to a network of **Insight Servers *w***hen broadcasting and receiving blockchain transaction information.

In essence, they are like nodes across a distributed network that handle transaction communication and keep track of updates to the various cryptocoin blockchain ledgers. They are operated by numerous different companies and groups (and *none of them by the Exodus company itself*). This helps guard against centralized "choke points" of failure.

Additionally, your transaction history is backed up to your Exodus wallet in an **encrypted format**; so *not even Exodus staff* can know how much money you've got stashed in your wallet. The result is a highly secure, redundant wallet that'll actually continue functioning perfectly fine even if the Exodus company were to go belly up!

However, *the trade-off* for this amazing degree of privacy and sovereignty is **personal responsibility**.

For example, Exodus staff simply cannot trace where transactions were sent without information YOU must first provide. Likewise, it is equally impossible for them to reset your password if you forget it.

Pro Tip: When it comes to your private keys...

- NEVER give them to a third party.
- NEVER broadcast them unencrypted across the web.
- Exodus staff will never ask for your private keys.
- No **legitimate** initial coin offering (ICO), airdrop or crypto-site will ever ask for them either.
- If some site DOES ask for your private keys: Give it a "one finger salute" and *leave quickly*, never to return again.

A New Frontier In Crypto Wallet Security

As a wallet, Exodus has made it extremely easy to keep your funds secure to the extent that *even if the Exodus company dissolves or is hacked*, your funds will still be safely and securely tucked away within YOUR wallet!

That said, while the Exodus wallet securely encrypts and protects your blockchain assets with a password, your Exodus wallet is only as secure as:

- The computer that it resides on,
- And the security practices of the user.

In other words, as covered in the previous section: You have to be *very cautious about things you download or websites you visit* via the computer containing your Exodus wallet (particularly if your wallet is open).

For example, malware and viruses are distributed by emails or malicious website links; whereby potentially containing key-logger spyware that sends your passwords or sensitive information to certain bad actors.

To maximize security, if you plan on holding certain blockchain assets and/or cryptocoins *in large quantity.*… consider various **long-term** strategies and solutions. So for Bitcoin, some viable options are:

- A multi-signature wallet like Copay,
- A high-security dedicated wallet client such as Electrum.
- A hardware wallet like the Ledger (Exodus is now in talks with hardware wallet providers for an *Exodus-compatible* hardware wallet solution).

Pro Tip: If approached correctly, another excellent layer of safety and security *for your entire Exodus wallet* (or any other installable crypto-wallet client, for that matter) is to set up a VirtualBox image with its own dedicated Linux install.

Once the VirtualBox image is created with a brand new (password-protected) Linux install, then install the Exodus wallet and **only** launch the VirtualBox image when you are actually going to be using your wallet *in real-time*. The moment you are done transacting with your wallet, shut down the VirtualBox image accordingly.

Honest Fees With Full Transparency

As previously mentioned in Part 1, blockchain-based networks such Bitcoin and Ethereum require a fee to send a transaction (aka "**TX fee**"). This fee does not go to Exodus, nor does Exodus mark up the TX fee; but rather it is paid *directly to the applicable network* to ensure transactions are delivered reliably and quickly.

Among other things, these TX fees help hwart spam transactions that would otherwise end up causing legit transactions to wait for hours (even days) due to network congestion. The more popular a network is, *the more expensive the TX fees tend to be* (in part why Bitcoin TX fees are utterly **astronomical** as compared to nearly all other blockchains).

Pro Tip: TX fees constantly fluctuate and are calculated on a combination of:

1. The amount of traffic the network currently has,
2. And the *size in bytes* of the transaction (i.e. the number of inputs and outputs).

They are **not** based on the "amount" of cryptocoin transacted; but specifically on the *amount of data sent* across the network.

A Simple Bitcoin Fee Example

Imagine having to *count out and roll up 100 pennies* to use as payment vs. simply handing over a one dollar bill: 100 pennies have the same "spending power" as a dollar bill, albeit they require a lot more effort to deal with.

So to put this into perspective, let's say that Alice receives 0.01 BTC every hour for 100 hours. Bob receives a payment of 1 BTC once. Both Alice and Bob now have a 1 BTC balance.

Yet if Alice and Bob were to coin-swap and send their 1 BTC to the other, Alice will have a **much** larger fee than Bob. This is because the Bitcoin network has to do a lot more work for Alice (in bundling all of her small "change inputs" together) vs. Bob who just has 1 input.

Unspent Transaction Outputs Demystified

Bitcoin (and similar blockchain protocols like Litecoin) store transaction data and user balances in the form of *unspent transaction outputs* (referred to as "**UTXO**"). They essentially boil down to a list of unspent amounts that have been sent **to** a user, but *not yet sent from them*. Hence the sum of these outputs is the user's total balance.

This is why individual bitcoins are easy to track. They are literally 'signed off' from one transaction to another; whereby Alice's transactions only become valid if she can prove ownership over the actual Bitcoin she is trying to send. In light of this, there was a lot of talk awhile back about Bitcoin being a gov experiment (particularly given Bitcoin's extremely murky historical roots).

However, many 2nd generation cryptocoins use a much more sensible "**account model**"; whereby decreasing transaction complexity and increasing fungibility. You can discover more on the pro's and con's of these two approaches here and here.

With all of that said, Exodus *always prioritizes speed and reliability over low fees* by dynamically tracking Bitcoin network congestion and adjusting fees accordingly. This ensures that all outgoing Exodus transactions are both fast AND at the best TX rate possible *every single transaction*!

Ethereum 'Smart Contract' Token Fees Demystified

Some of the supported assets within Exodus are ERC20 tokens powered by Ethereum.

This means that there are *additional fees* above the typical TX fee associated with an outgoing transaction (i.e. sending to a 'smart contract' address).

To ensure that your ERC20-based transactions always get processed in a timely manner...

Exodus **requires** you to keep a minimum of **0.015 ETH** in your Exodus wallet, as a buffer against Ethereum's ever-increasing network fees (0.3 ETH is recommended).

If you've never played around with a token-based asset that rides on top of a cryptocoin... at first glance, it might make no sense as to why Exodus requires a minimum amount of Ethereum just to be able to wheel and deal in ERC20 tokens and such.

In short, ERC20 tokens are likened to a vehicle and Ether (ETH) is the “fuel” that powers these assets across the Ethereum network (covered fully in Part 3). Hence if you have have an Ethereum-powered asset and no Ether... it’s like a car without gas. So here’s what you’ll need to do if you want to play around with ERC20 tokens:

Either...

1. Exchange any other cryptocoin for at least 0.015 ETH inside your Exodus wallet. Once the exchange is complete, and your Ethereum is deposited, you can begin to manage and/or exchange Ethereum-powered assets.

Or…

2. Deposit ETH into your Exodus wallet from an outside source (i.e. external wallet or exchange).

Pro Tip: Ethereum TX fees *further increase* if you send them to a 'smart contract' address. Smart contracts are programs that automatically perform tasks; usually involving ERC20 assets and/or managing Ethereum funds. For example, some exchanges use them for their deposit addresses.

The fees are higher so as to ensure that the smart contract has enough 'fuel' to move the transaction AND execute the actual smart contract itself. Sending a transaction with sub-optimal fees to a smart contract often results in a failed transaction.

At this writing, Ethereum TX fees are usually (but not always) significantly lower than an equivalent Bitcoin transaction. Exodus *automatically adjusts the final fee* to compensate for assets sent to a smart contract, thus ensuring that your transactions get processed onto the blockchain in a timely manner.

How Exodus Makes Money

Exodus generates revenue from a portion of the spread on asset exchanges; hence Exodus is proud to have **100% transparency** on all cryptocoin exchanges made through the Exodus wallet.

In a nutshell:

- Highly liquid markets have tighter spreads (i.e. lower percentages).
- Conversely, low-liquidity markets have higher spreads (i.e. higher percentages) due to *low trade volume*.
- This is why high-liquidity market pairs like Bitcoin/Ethereum have a *noticeably lower fee* than a much less popular market pair.

Although spreads can vary greatly based on market conditions, typical strong-liquidity spreads range between 2-4% or less. The exact amount and rate you’re getting will be always listed on the *exchange section* of the wallet. For your convenience, asset values in approximate local currency are also listed right alongside the market pairs; whereby making it a breeze to estimate fiat costs.

All Of That Said… A Caveat Is In Order:

Because Exodus exclusively utilizes ShapeShift specifically for the exchange feature, fees tend to be **rather hefty** considering that ShapeShift's fees are already pricey to begin with (as compared to a major exchange like Binance). Even ShapeShift's main competitor Changelly charges *way lower fees* (albeit still pricey compared to Binance),

Now you can make an informed decision accordingly… "convenience vs. cost savings".

How The Exodus Exchange Works

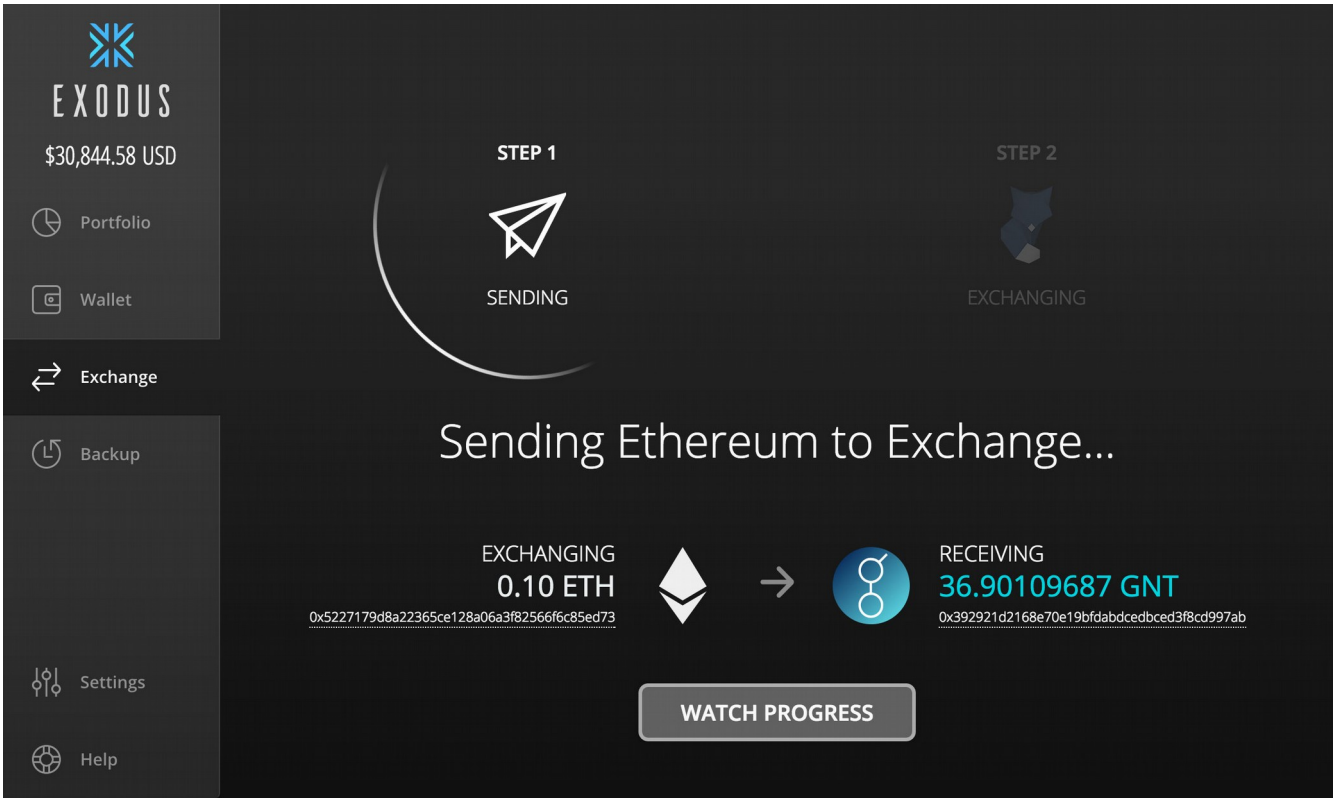
Admittedly, Exodus does in fact make exchanging cryptocoins easy-peasy: Simply click the coins you want to exchange, choose the amount, and confirm the transaction. All the dirty little details of the exchange are seamlessly dealt with behind the scenes.

Once an exchange begins, Exodus sends your assets to their exchange partner ShapeShift. ShapeShift then processes your deposit and sends back your converted assets shortly thereafter (at least in theory).

However, Exodus does show this process in **two steps**, with a handy spinning activity circle highlighting your current progress as the exchange takes place:

Step 1: Sending

- This is the first step once the exchange begins. During step 1 Exodus initiates the exchange order with ShapeShift. This step typically takes under a minute.
- Once this step is complete, and the progress circle moves to step 2, you will see your Exodus balance temporarily decrease for the amount of your exchange.
- During this time, you'll relinquish possession of your coins; whereby your Exodus balance reflects this decrease whilst waiting for the exchange to complete.



Step 2: Exchanging

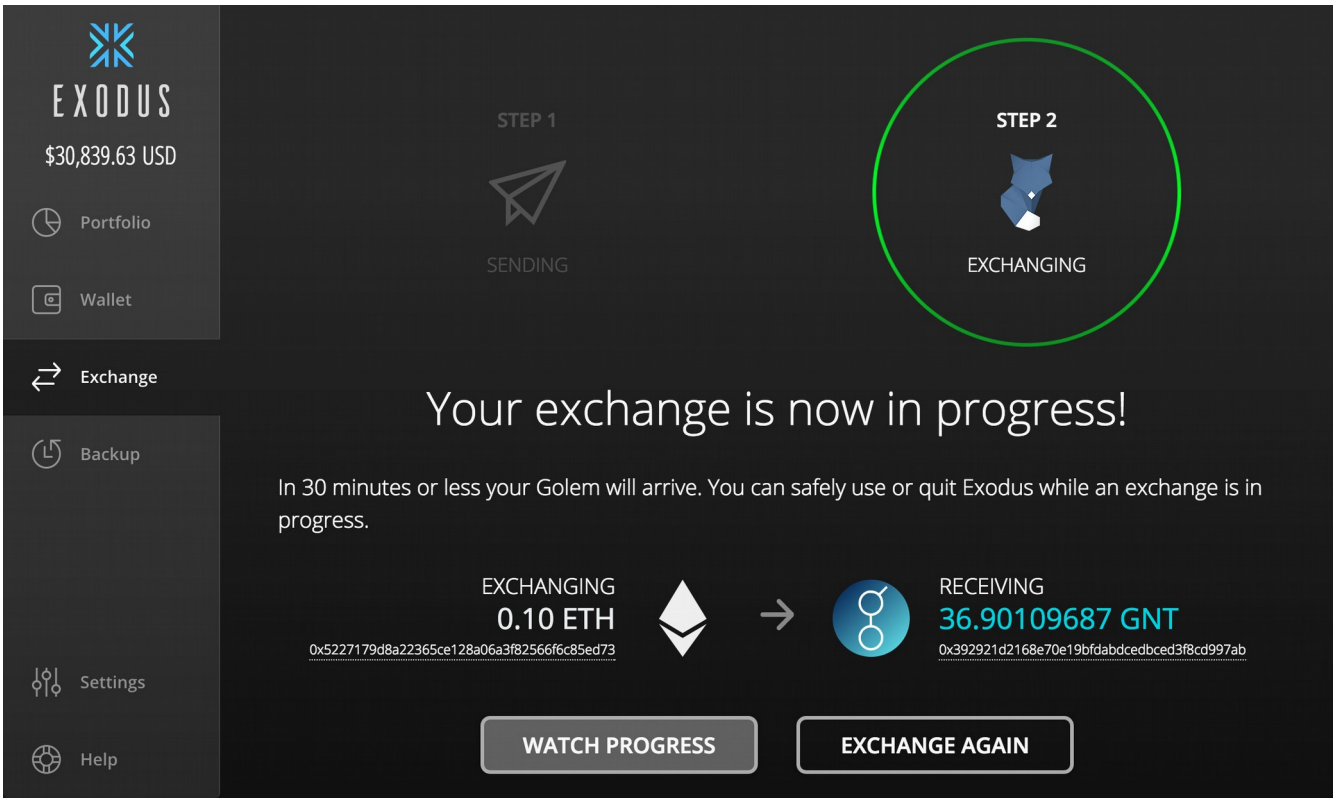
This is the second step in the exchange. This process takes the longest, as each asset has a *blockchain settlement time* that typically ranges from a couple minutes up to an hour (assuming normal network congestion for both coins involved in the exchange).

Although it can be unnerving at times, this process is perfectly normal. Your balance will eventually jump back up again once the exchange is complete and your new assets are deposited into your wallet.

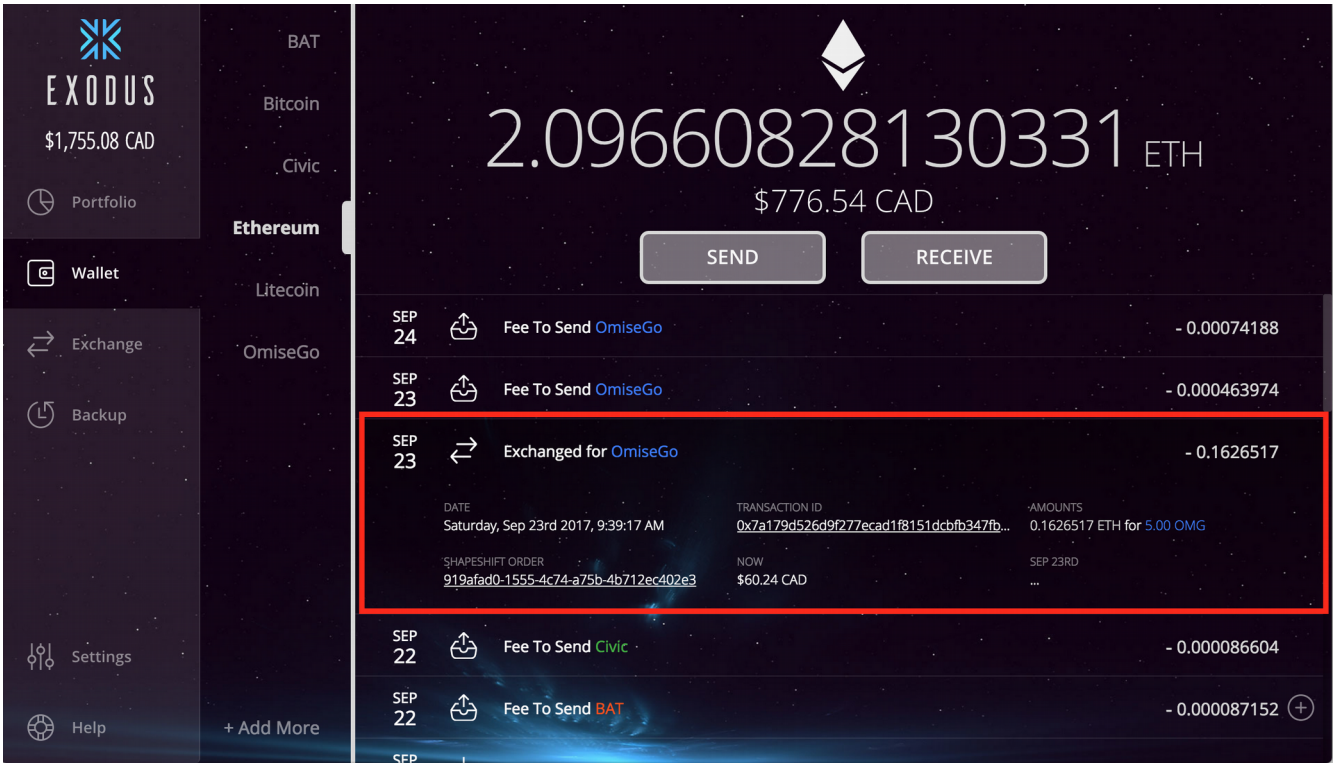
For example, exchanging **into BTC** (regardless of what coin was exchanged) typically takes the longest; whereas exchanging into fast-settling altcoins such as Litecoin or Ethereum sometimes only take a couple minutes. Overall exchange wait time is largely based on 1) each coin's typical settlement time, and 2) overall network congestion for both cryptocoins involved.

Examples:

- If you exchange Bitcoin for Ethereum, you'll typically wait 15-60 minutes (leaning toward an hour).
- Conversely, if you are exchanging Ethereum for Bitcoin, your typical wait is less than 30 minutes (often times, much less).



Pro Tip: If you want to see details of your exchange click on “Wallet”, then on the asset you sent in to exchange. You will see a transaction line item you can click to expand and see details about the exchange, including exchange rate, transaction ID, and Shapeshift exchange order ID:



General Tips For Exchanging Assets In Exodus

- You can safely continue using and/or exchanging in Exodus while an exchange is in progress.
- If you don’t have time to wait for an exchange to finish simply quit Exodus and go about your business. 30-60 minutes later (for BTC, and even less for altcoins in most cases) simply re-launch Exodus and your new assets should now be available in your wallet.

Pro Tip: Exodus claims to supposedly exchange in excess of USD$1M+ daily with no loss of customer funds. Nonetheless, if there is EVER a problem with their partner ShapeShift, Exodus will personally ensure you are taken care of ASAP. You can read up on the procedure explainer here.

Given ShapeShift’s alarming track record, this can be very reassuring indeed.

Exodus-Supported Blockchain Assets

You can see what additional assets have been added since here. And while certain Ethereum Assets (including *DigixDAO, Tron, VeChain, Icon, Binance Coin, Dragonchain* and others) can also be safely stored, sent and received… they are **NOT** supported for exchange within Exodus.

Supported Assets

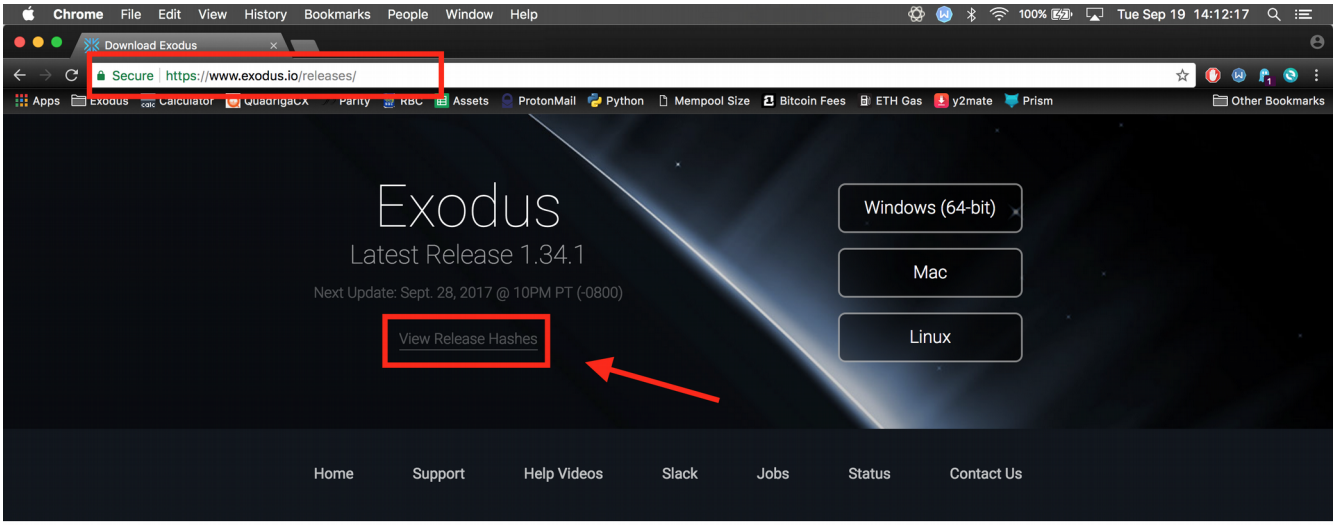
ASSET	DATE SUPPORTED
Bitcoin (BTC)	Dec. 9, 2015
Litecoin (LTC)	Dec. 9, 2015
Ethereum (ETH)	Feb. 12, 2016
Dash (DASH)	Apr. 8, 2016
Golem (GNT)	Apr. 14, 2017
Augur (REP)	Apr. 27, 2017
Decred (DCR)	Jun. 22, 2017
EOS (EOS)	Jul. 6, 2017
Aragon (ANT)	Jul. 6, 2017
Gnosis (GNO)	Jul. 20, 2017
OmiseGo (OMG)	Aug. 17, 2017
Basic Attention Token (BAT)	Aug. 31, 2017
Civic (CVC)	Sep. 15, 2017
SALT(SALT)	Sep. 25, 2017
Bitcoin Cash (BCH)	Oct. 12, 2017
Ethereum Classic (ETC)	Oct. 12, 2017
FunFair (FUN)	Oct. 26, 2017
District0x (DNT)	Oct. 26, 2017
Bancor (BNT)	Jan. 19 2018
Bitcoin Gold (BTG)	Jan. 19 2018
Edgeless (EDG)	Jan. 19 2018
FirstBlood (1ST)	Jan. 19 2018
Matchpool (GUP)	Jan. 19 2018
Numeraire (NMR)	Jan. 19 2018
iExec RLC (RLC)	Jan. 19 2018
Status (SNT)	Jan. 19 2018
WeTrust (TRST)	Jan. 19 2018
Wings (WINGS)	Jan. 19 2018
0x (ZRX)	Jan. 19 2018
Vertcoin (VTC)	Feb. 15 2018
Metal (MTL)	Feb. 15 2018
SingularDTV (SNGLS)	Feb. 15 2018
Storj (STORJ)	Feb. 15 2018
Ripio (RCN)	Mar. 16 2018
One-Click EOS Registration	Mar. 29 2018
Digibyte (DGB)	Apr. 12 2018
Zcash (ZEC)	Apr. 26 2018

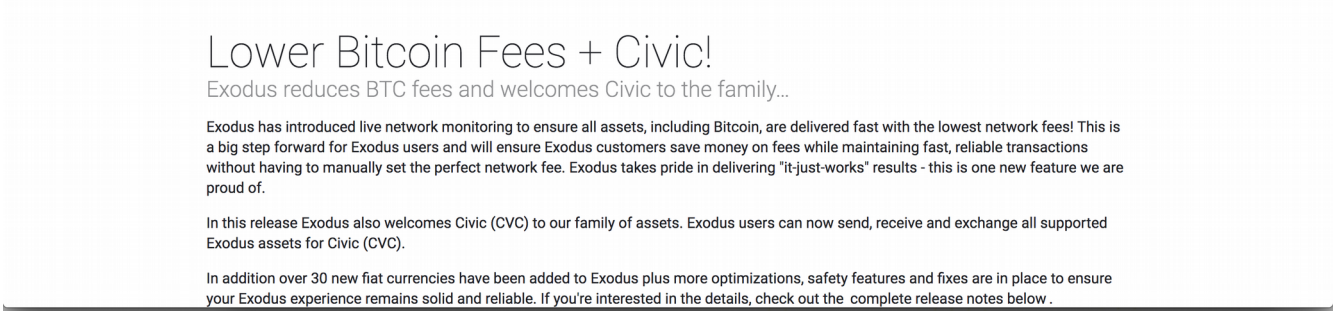
Getting Started With Exodus

There are two main steps to getting up and running with Exodus:

Step 1: Download & Install Exodus

- **Step 1a:** Watch the short tutorial specific to your OS: Mac, Linux, Windows.
- **Step 1b:** Download Exodus directly off of Exodus.io (Always check your URL bar and confirm the source before downloading anything off the web!)
- **Optional Yet Highly Recommended Step 1c:** Verify authenticity of downloaded file before installing. On the official Exodus download page, you'll find the link to the PGP signed hashes of each installer:





Lower Bitcoin Fees + Civic!

Exodus reduces BTC fees and welcomes Civic to the family...

Exodus has introduced live network monitoring to ensure all assets, including Bitcoin, are delivered fast with the lowest network fees! This is a big step forward for Exodus users and will ensure Exodus customers save money on fees while maintaining fast, reliable transactions without having to manually set the perfect network fee. Exodus takes pride in delivering "it-just-works" results - this is one new feature we are proud of.

In this release Exodus also welcomes Civic (CVC) to our family of assets. Exodus users can now send, receive and exchange all supported Exodus assets for Civic (CVC).

In addition over 30 new fiat currencies have been added to Exodus plus more optimizations, safety features and fixes are in place to ensure your Exodus experience remains solid and reliable. If you're interested in the details, check out the complete release notes below.

Installation Notes: Exodus will only run on **64 bit** systems. Also, **Windows 7 Users** need to ensure that .NET Framework **4.5.2** is installed. If it is not installed prior to installing Exodus wallet, the installer will attempt to do it for you.

Worst Case: If the automatic .NET install fails, simply download the .NET installer from the Microsoft website and install it yourself, then relaunch the Exodus installer and it should install just fine.

Step 2: First Transaction & Backup

Now that you've got the Exodus wallet up and running, you need to "seed" it. To do so only requires that *a small amount of cryptocoin slightly greater than the TX fee* be sent to your brand new wallet (any supported coin will work fine).

This first inbound Exodus transaction is important because when Exodus receives your first deposit, it will allow you to view your wallet "seed" (your secret 12-word mnemonic passphrase that functions as the "master key" to all of your assets).

This passphrase *unlocks the full power of Exodus*; whereby allowing you to access your balance from anywhere (or even transfer all your funds to another wallet if you so choose). So **write it down on real paper and store it safely offline.**

You will then be asked to create a password for your wallet. Please choose a password that is:

- Different from any other password on your computer.
- And ideally **at least 12+** characters; containing no recognizable words, and at least one upper and lower case, one number, and one special character.
- You also have the option to create an email backup that allows you to *restore your funds from your password*.

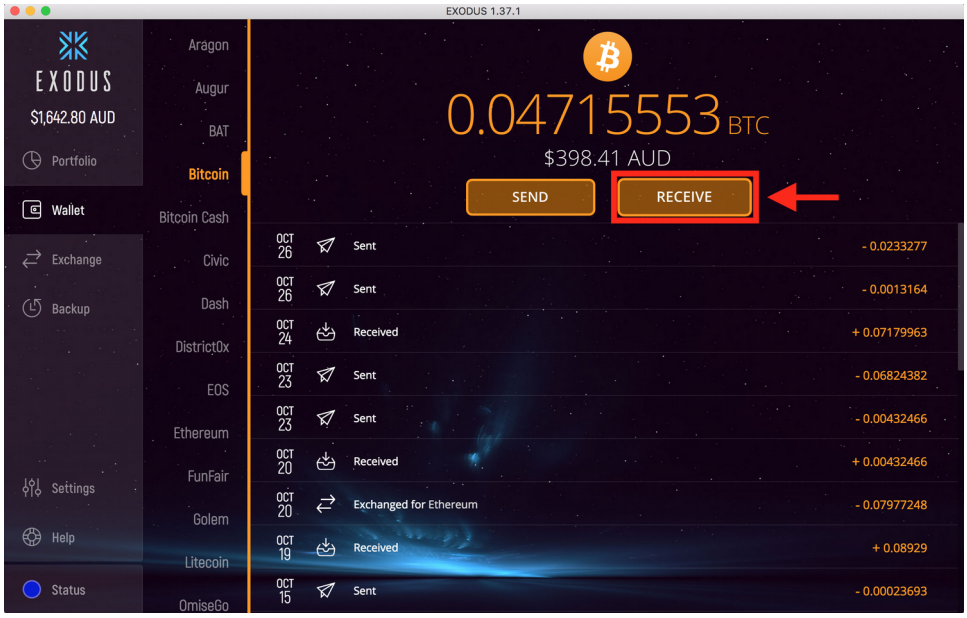
This backup is your 12-word recovery phrase encrypted in a URL with your password. It is important to note that Exodus does not store your keys on their servers. So even if the Exodus site is hacked, your funds are perfectly safe. However, this also makes keeping your keys safe **YOUR responsibility**.

Hence why making an email backup and physically writing down your 12-word passphrase are both very important: It gives you t**wo methods** for restoring your wallet.

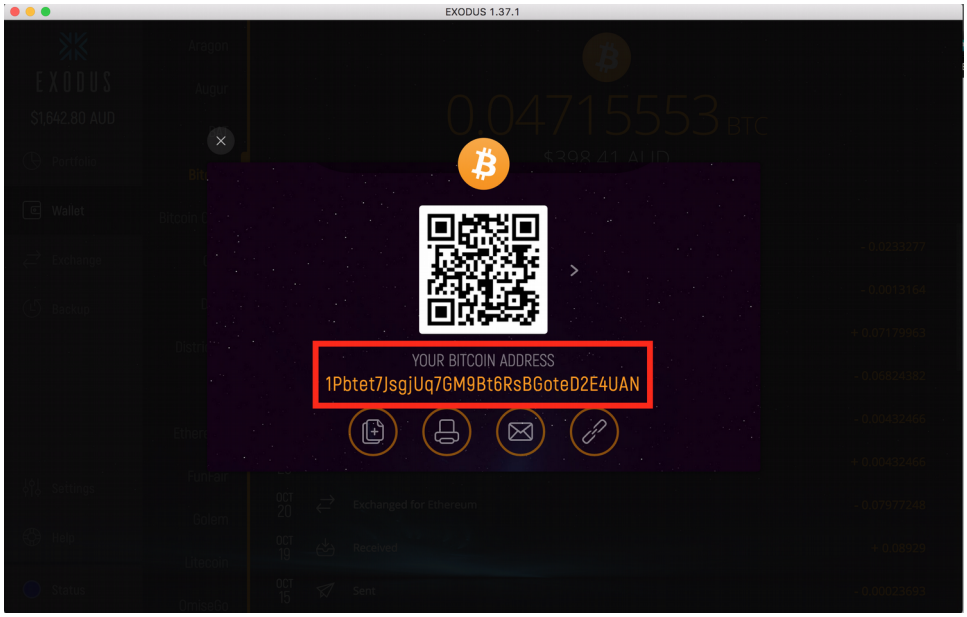
Making Your First Transaction

These instructions work for receiving *any blockchain asset* supported by Exodus. Start by clicking "Wallet" on the left sidebar. Then choose the blockchain asset you would like to receive.

In this example, we'll click Bitcoin, then the Receive button:

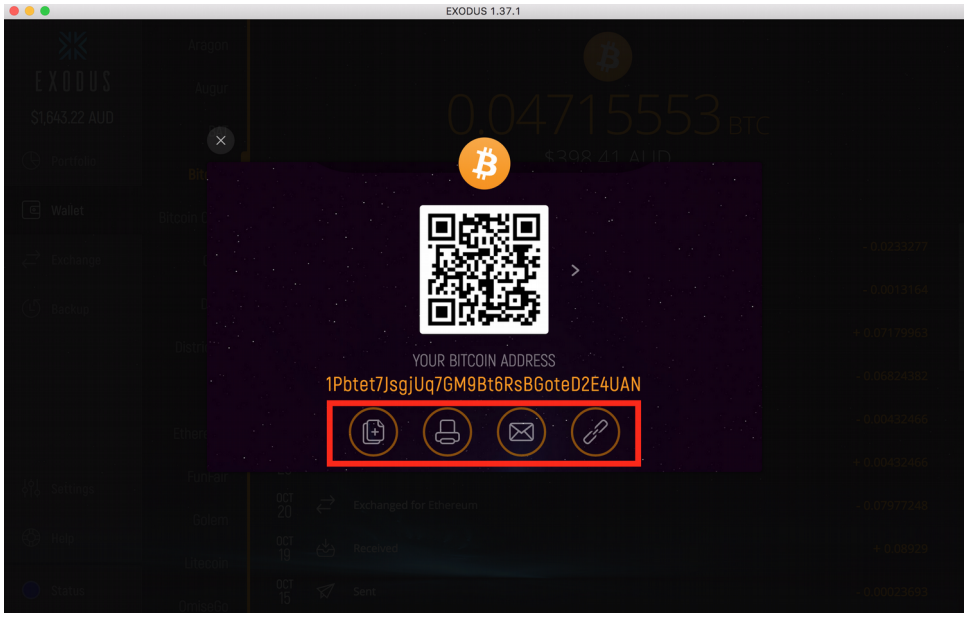


Once you click the receive button, Exodus shows your BTC address. Similar to a bank account number, you give this QR code or address to another person/wallet you want to receive a BTC payment from.



There are four action buttons in this window to copy, print, and email your BTC address, as well as view your address on the blockchain.

Finally, there is a QR code in this window that contains your BTC address. Simply scan this QR code from a mobile device to send BTC between devices without typing long addresses or emailing blockchain addresses to yourself.



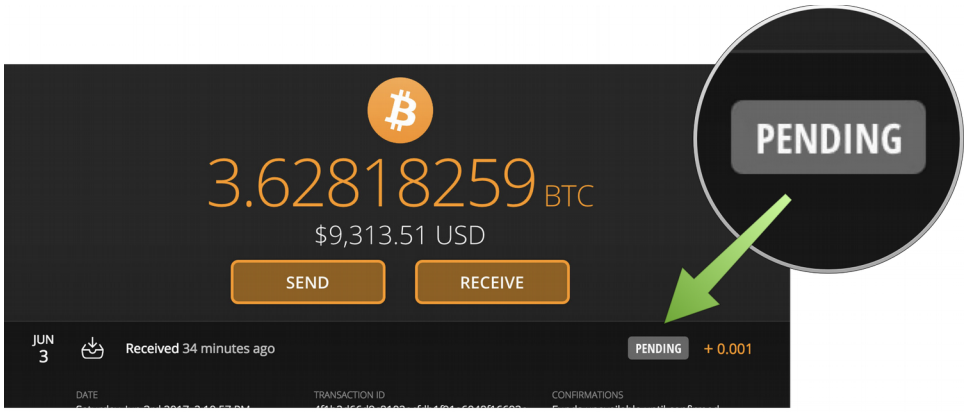
Pro Tip: If you don't already have some crypto to start with, here are several other possibilities. You may well also have local opportunities or perhaps even a Bitcoin ATM within your area.

Once you've had a chance to familiarize yourself with Exodus' basic functions, the next thing you'll want to familiarize yourself with is...

How To Track Your Exodus Transactions

Since your main Exodus activities involve sending and receiving transactions, it's wise to know *how to track your transactions* in Exodus. Exodus transactions can either be 'Unconfirmed', 'Pending', or 'Confirmed'

The time it takes for a transaction to complete depends on the asset traded, the fee used by the sender, and the overall network congestion of both coins. However, once a transaction is verified, the Pending tag will be removed. This lets you know the transaction cannot be reversed and the funds can be sent:



This verification process is similar to the 2-5 day hold traditional banks put on check deposits waiting for funds to clear. Blockchains have a similar system, except the downtime is reduced to mere hours *or oftentimes, even minutes* (with faster networks like Golem) instead of days:

Asset:	**Typical Pending Time:**
Bitcoin	60 minutes or less
Dash	15 minutes or less
Decred	15 minutes or less
Ethereum	5 minutes or less
Golem	5 minutes or less
Augur	5 minutes or less
Litecoin	15 minutes or less

Occasionally, transactions are not accepted by the network and remain marked as 'Pending' for an *uncharacteristically long* period of time. When this happens, these transactions will rarely ever confirm due to one of three main reasons:

- **Receiving a transaction with insufficient TX fees.** All transactions require a TX fee in order to be confirmed by the asset network. If the sender specifies a insufficient fee (or none at all), then the transaction may well never confirm.

- **Spending unconfirmed assets.** If you are trying to send assets that appear as pending in your account, your transaction will also remain in a pending state until your deposits are confirmed.

- **The network is experiencing high volume.** Sometimes there is a high volume of digital currency being sent globally, and there are more transactions than there is space available in each new block to include the transaction.

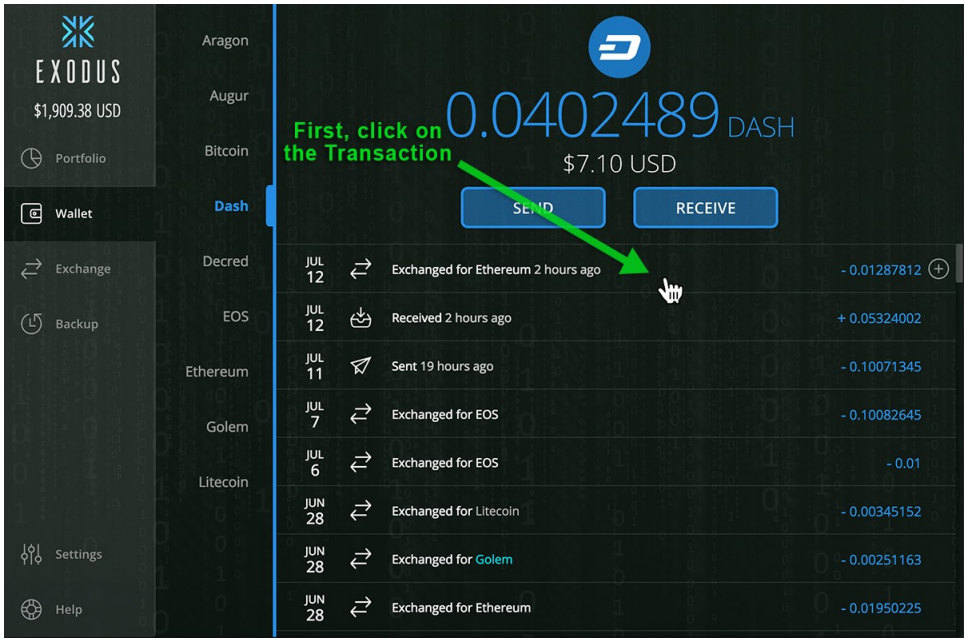
If you have a “stinker transaction” in your account that has remained pending much longer than reasonably expected, you can do a direct look-up *on the blockchain itself* to see what’s really going on.

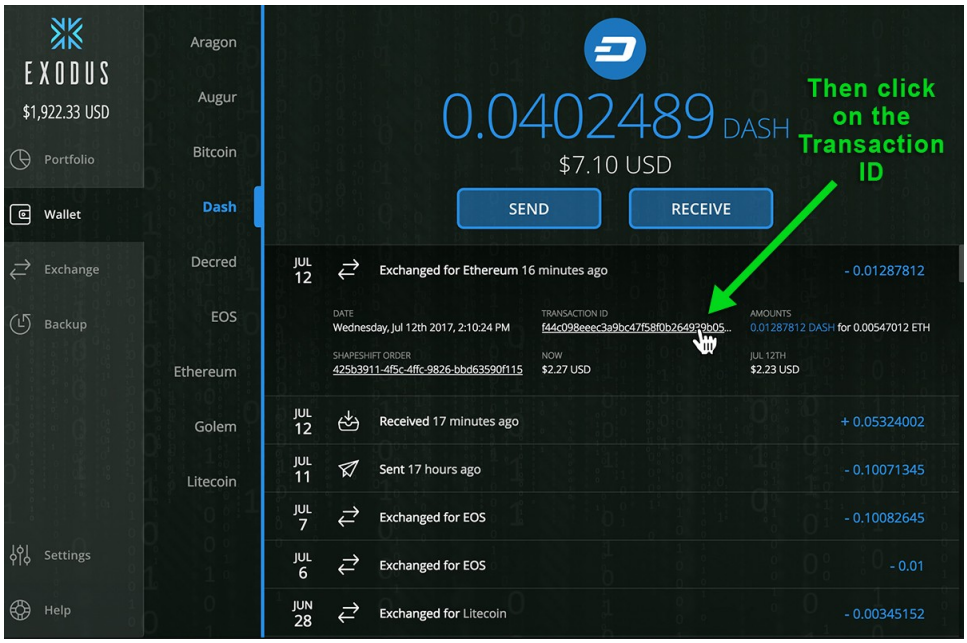
How To Track Your Exodus Transactions Directly On The Blockchain

To see if a transaction was actually broadcast correctly, you can look up the status of your transaction directly on the blockchain *from inside Exodus.*

Click on any Transaction ID, and it will bring you to a blockchain explorer (a site that allows you to look at your transaction and its state; including number of confirmations and the public addresses involved in this transaction).

This is a simple and convenient way to troubleshoot why certain transactions are seemingly misbehaving:





This will take you to a blockchain explorer showing the details of the transaction.

Pro Tip: If you ever need to elicit the help of the Exodus support team on a specific transaction...

For **fastest response**: 1) copy the URL of the blockchain explorer page that you were directed to (as shown above) AND 2) your ShapeShift Order ID for the transaction in question, and send them to support@exodus.io. These two info's will help get you squared away much more quickly.

What To Do When Your Exodus Wallet Disagrees With The Blockchain

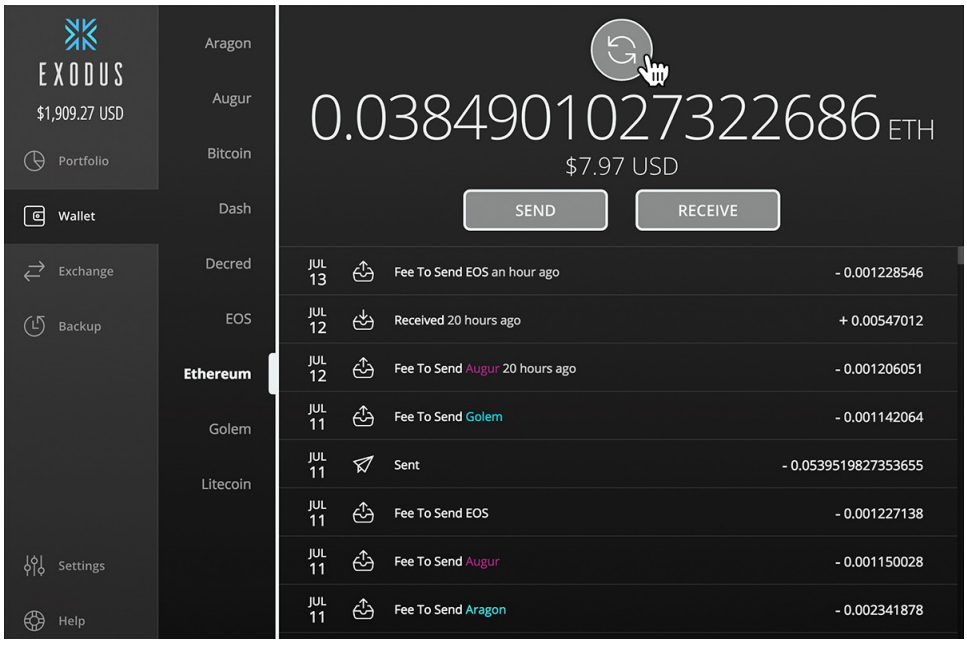
When Exodus shows the funds in your wallet to be lower/higher than what the blockchain shows... fret not: **The blockchain is always right**. This simply lets you know that your Exodus wallet is *out of sync* with one or more of the blockchain networks.

Other phenomena that may be indicative of an unsynchronized wallet in need of *manual refreshment* also include...

- Running into a major network problem,
- Getting a sending error when you normally shouldn't,
- Exodus just closes down on you unexpectedly for no apparent reason.

A quick asset refreshment oftentimes fixes a number of asset-related problems simultaneously. Below is an example of how to refresh Ethereum. However, the steps are the same for all assets:

1. Open your Ethereum wallet by clicking on "Wallet" on the left sidebar then choose "Ethereum".
2. Mouse over the Ethereum logo and you will see a refresh icon. Click on the refresh icon.
3. A dialog asks you if you want to rescan the blockchain. Choose "Rescan".



When this process starts, individual transactions are counted and rebuilt (similar to reorganizing a messy receipt box). When the refresh icon is finished spinning, all your transactions will be freshly updated and synced.

Note: This feature was *vastly improved* in version 1.41. So if you are still using an older version, update to the latest version of Exodus, then follow the steps above for each coin you hold.

Most of the time, this solves the display issue and you are good to go. If it does not, the issue may well be with your *web connection* itself. Try rebooting your computer, router and/or change your network to solve the issue. If none of these work, then the Exodus support team will happily help you!

Staying Up To Date With Exodus

Exodus makes it really convenient to stay in touch:

- **Exodus Wallet Roadmap:** https://support.exodus.io/article/96-exodus-wallet-roadmap
- **Slack:** https://exodus-invite.herokuapp.com/
- **Instagram:** https://www.instagram.com/exodus_io/
- **Twitter:** https://twitter.com/exodus_io/
- **Github:** https://github.com/ExodusMovement
- **Vimeo:** https://vimeo.com/exodusio
- **YouTube:** https://www.youtube.com/channel/UCpwUeFzkWEEduSoxpiI1UsA
- **Support Email:** support@exodus.io